UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

ALEXIS HUERTA, Plaintiff, vs. T-MOBILE USA, INC., Defendant.	NO. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Alexis Huerta ("Plaintiff"), by and through his undersigned attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant T-Mobile USA, Inc. ("T-Mobile"), and makes the following allegations based upon knowledge as to himself and his own acts, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This is a class action brought by Plaintiff individually and on behalf of all other similarly situated individuals whose personal information, including names, drivers' license numbers, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs, addresses, and phone numbers (hereinafter "Personal Information" or "PI") was stolen from T-Mobile in 2021 (the "Data Breach").

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

2. On August 17, 2021, T-Mobile learned that hackers had accessed the Personal Information of tens of millions of customers. While T-Mobile has reported that its investigation is ongoing, since the original announcement T-Mobile has continued to discover that some customers also had exclusive and valuable PIN numbers stolen that can permit cybercriminals to easily assume a person's identity and takeover control of their personal email, financial, and other online accounts that use two-factor authentication by sending access codes to their cell phones. Even worse, T-Mobile has been subject to many recent data security incidents and it has been reported that cybercriminals have been offering the recently stolen data for sale.

3. As a result of Defendant's misconduct, the Data Breach compromised the PI of tens of millions of Americans entrusted to it. Victims have had their PI compromised, their privacy violated, are at an increased risk of exposure to fraud and identity theft, have suffered a loss of control over their personal and financial information, and have otherwise been injured. Through this suit, Plaintiff and the Class seek to recover damages caused by Defendant's breaches of common law duties and violations of state and federal consumer protection statutes. Plaintiff also seeks injunctive and declaratory relief on behalf of himself and similarly-situated Class members.

II. PARTIES

4. Plaintiff Alexis Huerta is an adult over the age of eighteen. He is a resident of Chula Vista, California. Plaintiff Huerta has been a T-Mobile cellular phone account holder for approximately nine years, and was notified by text message by T-Mobile that his Personal Information was compromised during the Data Breach. Plaintiff Huerta has also been recently subject to attempted identity fraud regarding his bank account through mobile apps. As a result of Defendant's failures to adequately safeguard Plaintiff's Personal Information, Plaintiff has been injured.

5. Defendant T-Mobile is a Delaware corporation with its corporate headquarters at 12920 Southeast 38th Street, Bellevue, Washington 98006. T-Mobile is a publicly traded

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

company (TMUS) that provides cellular phones and data plans to consumers throughout the United States.

III. JURISDICTION AND VENUE

6. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

7. This Court has personal jurisdiction over T-Mobile because its headquarters are in this District and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part from this District.

8. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant is a resident of and does business in this District, has intentionally availed itself of the laws and markets within this District by conducting substantial business in this District, and a significant portion of the facts and circumstances giving rise to this Complaint occurred in or emanated from this District and the State of Washington.

IV. FACTUAL ALLEGATIONS

A. Background.

9. T-Mobile is company that sells cellular phones made from manufacturers like Apple and Samsung directly to consumers throughout the United States in its retail stores. It is a subsidiary of the German telecommunications conglomerate Deutsche Telekom AG. T-Mobile claims to have the "first and largest nationwide 5G network" that "reaches more cities and towns in America than anyone else." T-Mobile provides wireless voice, messaging, and cellular telephone services and data plans for wireless devices including smartphones, tablets, and wearables. Many of these plans are subject to subscription plans and some are "pre-paid"

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

for certain amounts of usage. T-Mobile reportedly has over 100 million U.S. customers and7annual revenues of over $15 billion.

10. T-Mobile states through its website that "our privacy principles mean you can trust us to do the right thing with your data." T-Mobile claims to be "open and honest about our privacy practices" and that "we're always working to protect you and your family and keep your data secure." In its current Privacy Policy for account holders, T-Mobile represents that "[w] use administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control." T-Mobile also notes that California consumers have additional "Personal Data Rights, including the right to access, delete, and stop the sale of personal data."

11. Despite these representations and agreements with consumers, T-Mobile failed to disclose that they did not maintain account holders' PI in compliance with state and federal mandated data security protocols, or even industry standards, in order to prevent the unauthorized access, use, and theft of PI.

B. The Data Breach.

12. On Sunday, August 15, 2021, news broke on the Internet that hackers were offering for sale the personal data of 100 million T-Mobile customers. Messages to Motherboard, a tech-based blog associated with Vice, confirmed that the PI came from T-Mobile's servers and included social security numbers, names, addresses, international mobile equipment identity ("IMEI")[1] and driver's license numbers—a veritable treasure trove of data highly attractive to cybercriminals for identify fraud. The proposed seller was apparently asking for 6 Bitcoin, the cryptocurrency favored for illicit transactions, that amounted to about $270,000, in exchange for 30 million social security numbers and indicated that they could sell more.

[1] An IMEI number is unique to each cellular phone and is used for features like blocking calls. It is permanent and cannot be changed.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

13. On Monday, August 16, 2021, T-Mobile publicly acknowledged the Data Breach, issuing a statement that: "We have been working around the clock to investigate claims that T-Mobile data may have been illegally accessed." T-Mobile stated it was cooperating with law enforcement and that: "We have determined that unauthorized access to some T-Mobile data occurred, however we have not yet determined that there is any personal customer data involved. We are confident that the entry point used to gain access has been closed, and we are continuing our deep technical review of the situation across our systems to identify the nature of any data that was illegally accessed."

14. The next day, T-Mobile began a series of announcements that demonstrated the scope and severity of the breach. On August 17, 2021, T-Mobile announced the breach impacted 7.8 million current customers and 40 million records of former or prospective customers. T-Mobile also confirmed the Data Breach included PI such as social security numbers, driver's license and government ID numbers, as well as names and contact information. T-Mobile emphasized that financial information, such as credit, debit, and payment information was not accessed and stolen. However, T-Mobile also announced that approximately 850,000 pre-paid customers had their PIN numbers exposed. This is a significant development because access to a PIN number can be used to have an account holder's phone calls and text messages be routed to another identity fraudster's phone (or more likely a "burner" used for crime and then discarded) so that password reset emails and text messages associated with financial account transactions would be rerouted unbeknownst to the impacted customer—allowing the thief to gain access to the customers bank and other accounts and make withdrawals or transactions.[2] T-Mobile began notifying impacted customers, telling them to change their PIN numbers and offering free identity protection services. Data security experts

[2] A reporter, Matthew Miller, who once had a similar theft of his cell phone PIN, ended up with the criminal accessing his Gmail account which was deleted (as well as his files in the cloud), and fraudulent Bitcoin transactions made in his Coinbase account. *See* https://www.cnet.com/tech/mobile/t-mobile-hack-and-sim-swap-fraud-how-to-prevent-your-phone-number-from-being-stolen/, last accessed Aug. 24, 2021.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

like Brian Krebs began warning consumers that the fallout of the breach could impact them for years and to be aware of phishing scams from criminals posing as T-Mobile itself.

15. By Friday, August 20, 2021, the scope of the Data Breach just kept growing, with T-Mobile issuing updated statements indicating at least 5.9 million more customer accounts were compromised.

16. On Thursday, August 26, 2021, John Binns, a 21-year-old American who moved to Turkey a few years ago, claimed responsibility for the Data Breach, informing the Wall Street Journal he managed to pierce T-Mobile's defenses after discovering in July an unprotected router exposed on the internet after scanning T-Mobile's known internet addresses for weak spots using a simple tool available to the public.[3] According to the Wall Street Journal, Mr. Binns "declined to say whether he had sold any of the stolen data or whether he was paid to breach T-Mobile."

17. The next day, on August 27, 2021, T-Mobile's CEO, Mike Sievert, published a public letter[4] regarding the Data Breach, admitting, "On August 17th we confirmed that T-Mobile's systems were subject to a criminal cyberattack that compromised data of millions of our customers, former customers, and prospective customers." Sievert confirmed "some SSN, name, address, date of birth and driver's license/ID information was compromised." T-Mobile has "notified just about every current T-Mobile customer or primary account holder who had data such as name and current address, social security number, or government ID number compromised. T-Mobile customers or primary account holders who we do not believe had that

---

[3] Drew FitzGerald and Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'*, WALL STREET JOURNAL (Aug. 26, 2021), https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105 (last visited Aug. 30, 2021).

[4] The Cyberattack Against T Mobile and Our Customers: What happened, and what we are doing about it., T-MOBILE.COM (2021), https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2021/The-Cyberattack-Against-T-Mobile-and-Our-Customers-What-happened-and-what-we-are-doing-about-it/default.aspx (last visited Aug. 30, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

data impacted will now see a banner on their MyT-Mobile.com account login page letting them know."

18. T-Mobile is no stranger to data security incidents. T-Mobile has been repeatedly hacked in the past three years alone, including:

- In January 2021, T-Mobile announced that it "recently discovered and shut down malicious, unauthorized access to some information" including phone numbers, account and call information for 200,000 customers;
- In March 2020, T-Mobile said hackers gained access to both its employees' and its customers' data, including account numbers, rate plans, and billing information—as well as social security numbers and financial account information;
- In November 2019, T-Mobile said hackers infiltrated PI such as names, billing, and contact information and encouraged impacted customers to change their PIN numbers; and
- In August 2018, T-Mobile apologized when 2 million customers' PI was exposed.

19. To date, T-Mobile's communications fail to comply with its obligation to provide adequate and timely notification of the Data Breach to impacted customers. T-Mobile is offering some impacted customers complimentary credit monitoring and identity protection services, but those services do not sufficiently protect those individuals from the threats data breaches pose and will not be in effect long enough to eliminate all potential damage from the Data Breach.

C. Industry standards, identity theft, and protection of personal information.

20. It is well known that PI, including social security numbers and account information in particular, is an invaluable commodity and a frequent target of hackers. Despite this widespread knowledge and industry alerts of other notable data breaches, T-Mobile failed to take reasonable steps to adequately protect its systems from being *repeatedly* breached.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

21. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[5]

22. T-Mobile is, and at all relevant times has been, aware that the PI it maintains is highly sensitive and could be used for illegal purposes by third parties. Indeed, T-Mobile's websites acknowledge that its customers expect adequate privacy, security and safeguards of its PI.

23. Consumers place a high value not only on their PI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[6]

24. Consumers are particularly concerned with protecting the privacy of their social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[7] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[8]

25. In light of the multiple high-profile data breaches targeting companies like Target, Capital One, Anthem, and Equifax, Defendant is, or reasonably should have been,

---

[5] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin, last accessed Aug. 24, 2021.

[6] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf, last accessed Aug. 24, 2021.

[7] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html, last accessed Aug. 24, 2021.

[8] Social Security Admin., Identity Theft and Your Social Security Number at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf, last accessed Aug. 24, 2021.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

aware of the importance of safeguarding their customers' PI, as well as of the foreseeable consequences of their systems being breached.

26. Nonetheless, and despite a history of failed protection of PI, T-Mobile failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

27. Defendant had a duty to Plaintiff and Class members to properly secure their PI, encrypt, tokenize, and maintain their PI using industry standard methods, use widely available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class members, and promptly notify Plaintiff and Class members when Defendant became aware of the potential that their customers' PI may have been compromised.

28. Plaintiff and Class members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of their PI, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and identity fraud, and a deprivation of the value of their PI.

29. Plaintiff and Class members have suffered and will continue to suffer additional damages based on the opportunity cost and time Plaintiff and Class members are forced to expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

V. CLASS ACTION ALLEGATIONS

30. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and a Nationwide Class defined as (the "Class"):

> All persons whose Personal Information was compromised in the Data Breach that was announced by T-Mobile in or around August 16, 2021.

31. Plaintiff further brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and members of the following class (the "California

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Subclass"):

> All persons residing in California whose Personal Information was compromised in the Data Breach that was announced by T-Mobile in or around August 16, 2021.

Excluded from the Class and California Subclass are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant has a controlling interest, and their current or former employees, officers, and directors; (3) counsel for Plaintiff and Defendant; and (4) legal representatives, successors, or assigns of any such excluded persons.

32. **Numerosity.** Though the exact number and identities of Class and California Subclass members are unknown at this time, Defendant has confirmed that tens of millions of individuals were affected by the Data Breach. Accordingly, the Class and California Subclass are so numerous that joinder of all members is impracticable.

33. **Commonality and predominance.** Common questions of law and fact exist as to all Class members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

a. Whether Defendant engaged in wrongful conduct as alleged herein;

b. Whether Defendant owed a duty to Plaintiff and Class members to adequately protect their Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiff and Class members, and whether Defendant willfully, recklessly, or negligently breached these duties;

c. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures to prevent unauthorized access to their data security networks and to Plaintiff's and Class members' Personal Information;

d. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

e. Whether Defendant failed to inform Plaintiff and Class members of the Data Breach in a timely and accurate manner;

f. Whether Defendant continues to breach their duties to Plaintiff and Class members;

g. Whether Defendant has sufficiently addressed or remedied Plaintiff's and Class members' injuries and have taken adequate preventive and precautionary measures to ensure that Plaintiff and Class members will not experience further harm;

h. Whether Defendant engaged in unfair or deceptive practices by failing to disclose that it failed to properly safeguarded Plaintiff's and Class members' Personal Information;

i. Whether Defendant violated the consumer protection statutes applicable to Plaintiff and members of the Class and California Subclass;

j. Whether Plaintiff and Class members suffered damages as a proximate result of Defendant's conduct or failure to act; and

k. Whether Plaintiff and Class members are entitled to damages, equitable relief, and other relief.

34. **Typicality.** Plaintiff's claims are typical of the claims of the Class and California Subclass he seeks to represent because Plaintiff and all members of the proposed Class and California Subclass have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Class and California Subclass.

35. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class and California Subclass, and has retained attorneys experienced in class actions and complex litigation as his counsel.

36. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class member, while

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Defendant economically feasible. Even if Class members could afford individual litigation, the court system could not. In addition to the burden and expense of managing many actions arising from the Data Breach, individual litigation increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

37. In the alternative, the proposed classes may be certified because:

a. the prosecution of separate actions by the individual members of the Class and California Subclass would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendant;

b. the prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class members, or which would substantially impair their ability to protect their interests; and

c. Defendant acted or refused to act on grounds generally applicable to the proposed classes, thereby making appropriate final and injunctive relief with respect to members of the Class and California Subclass as a whole.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE

38. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

39. Plaintiff and Class members entrusted Defendant with highly sensitive and inherently personal private data subject to confidentiality.

40. In requiring, obtaining and storing Plaintiff's and Class members' Personal Information, Defendant owed a duty of reasonable care in safeguarding this PI.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

41. Defendant's networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class members' Personal Information was secured from release, disclosure, and publication.

42. Defendant's networks, systems, protocols, policies, procedures and practices were not reasonable given the sensitivity of the Plaintiff's and Class members' PI.

43. Upon learning of the Data Breach, Defendant should have immediately reported the Data Breach to Plaintiff and Class members, credit reporting agencies, the Internal Revenue Service, financial institutions, and all other third parties with a right to know and the ability to mitigate harm to Plaintiff and Class members.

44. Despite knowing their networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class members' PI were secured from release, disclosure, and publication, Defendant ignored the inadequacies and were unmindful of the risk of release, disclosure, and publication it had created.

45. Defendant's behavior evidences a reckless disregard for Plaintiff's and Class members' rights. Defendant's negligence is directly linked to Plaintiff's and Class members' injuries.

46. As a result of Defendant's reckless disregard for Plaintiff's and Class members' rights by failing to secure their Personal Information despite knowing their networks, systems, protocols, policies, procedures, and practices were not adequately designed, implemented, maintained, monitored, and tested, Plaintiff and Class members suffered injury, including but not limited to the impermissible release, disclosure, and publication—both directly and indirectly by Defendant as well as unauthorized parties—of their Personal Information as well as exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class members must monitor their financial accounts and credit histories more

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

closely and frequently. Plaintiff and Class members have also incurred and will continue to incur costs for the time and expense necessary to obtain credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The impermissible release, disclosure, and publication of Plaintiff's and Class members' PI has also diminished the value of their PI.

47. The harm to Plaintiff and the Class members was a proximate and reasonably foreseeable result of Defendant's breach of their duty of reasonable care in safeguarding Class members' Personal Information.

48. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

49. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

50. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, the California Customer Records Act, Civ. Code §§ 1978.80, *et seq*., and other similar state laws, Defendant had a duty to provide adequate data security practices to safeguard Plaintiff's and Class members' PI. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

51. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of its duties and legal requirements. Defendant knew or should have known, particularly in light of prior breaches, that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their PI.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

52. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members face an increased risk of future harm and have incurred damages.

53. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

54. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

55. Defendant provides cellular phone and data services to Plaintiff and Class members in accordance and subject to the terms of their privacy policies and practices. As consideration, Plaintiff and Class members paid money and/or provided PI to Defendant. Accordingly, Plaintiff and Class members paid Defendant to properly maintain and store their PI and not disclose it to unauthorized third parties. Defendant violated its implied contracts by failing to employ reasonable and adequate privacy practices and measures, leading to the disclosure of Plaintiff's and Class members' PI for purposes not required or permitted under the policies.

56. Plaintiff and Class members have been damaged by Defendant's conduct, including by paying for services, privacy, and data security practices they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

FOURTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT— DECEPTIVE BUSINESS PRACTICES, RCW 19.86, *ET SEQ.*

57. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

58. Defendant is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1), and conducts "trade" and "commerce" within the meaning

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

of the Washington Consumer Protection Act, RCW § 19.86.010(2).

59. The conduct alleged in this Complaint is deceptive within the meaning of the Washington Consumer Protection Act, RCW 19.86.010, *et seq*. Defendant did not disclose their failure to take reasonable steps to protect the security of Plaintiff's and Class members' Personal Information. Defendant also failed to timely and adequately disclose the Data Breach.

60. Defendant's omissions had the capacity to deceive a substantial portion of the public and have impacted the public interest and injured Plaintiff and the Class.

61. Defendant's omissions are material to reasonable consumers like Plaintiff and Class members because reasonable consumers place a high value not only on their Personal Information, but also on the privacy of that data.

62. Defendant's deceptive acts or practices have repeatedly occurred in trade or commerce within the meaning of the CPA, RCW 19.86.010(2) and RCW 19.86.020.

63. The acts complained of herein are ongoing or have a substantial likelihood of being repeated.

64. Defendant's deceptive acts or practices impact the public interest because they injured Plaintiff and Class members and have the capacity to injure millions more.

65. As a result of Defendant's deceptive conduct, Plaintiff and the Class are entitled to recover damages from Defendant in an amount to be proven at trial. Furthermore, pursuant to RCW § 19.86.090, Plaintiff and the Class are entitled to trebling of their proven damages.

66. Plaintiff and the Class are also entitled to an award of attorneys' fees pursuant to RCW § 19.86.090.

67. Plaintiff and the Class are entitled to an order, *inter alia*, declaring Defendant's conduct unlawful, and permanently enjoining Defendant from further violations of the Consumer Protection Act.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

FIFTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT—UNFAIR BUSINESS PRACTICES, RCW 19.86, *ET SEQ*.

68. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

69. Defendant is a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010(1), and conducts "trade" and "commerce" within the meaning of the Washington Consumer Protection Act, RCW § 19.86.010(2).

70. The conduct described in this Complaint is unfair within the meaning of the Washington Consumer Protection Act, RCW 19.86.010, *et seq*. Defendant knew and should have known that Plaintiff's and Class members' Personal Information is highly sensitive and could be used for illegal purposes by third parties. Nonetheless, Defendant did not adequately safeguard the data entrusted to them and failed to implement even the most basic data security protocols, making the data vulnerable to hackers. Defendant also failed to timely and adequately disclose the Data Breach to consumers.

71. Defendant's acts or practices are unfair because they: (1) caused injury to Plaintiff and Class members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

72. Defendant's acts or practices are also unfair because they are immoral, unethical, oppressive, or unscrupulous.

73. Defendant's unfair acts or practices have repeatedly occurred in trade or commerce within the meaning of the CPA, RCW 19.86.010(2) and RCW 19.86.020.

74. The acts complained of herein are ongoing or have a substantial likelihood of being repeated.

75. Defendant's unfair acts or practices impact the public interest because they injured Plaintiff and Class members and have the capacity to injure millions more.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

76. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiff and Class members suffered injury.

77. Plaintiff and Class members are therefore entitled to legal relief against Defendant, including recovery of actual damages, treble damages, attorneys' fees, costs of suit, and such further relief as the Court may deem proper.

78. Plaintiff and Class members are also entitled to injunctive relief in the form of an order prohibiting Defendant from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate, including but not limited to, disgorgement, for the benefit of Class members, of all or part of the ill-gotten profits received from Defendant's unlawful practices.

SIXTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON DATA BREACH LAW, RCW 19.255, *ET SEQ.*

79. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

80. The Washington Data Breach Law provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." RCW § 19.255.010(2).

81. The Data Breach resulted in the "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, who therefore experienced a "breach of the security of [their] system[s]," as defined by RCW § 19.255.010(4).

82. Defendant failed to disclose that the Personal Information of over 100 million customers had been compromised immediately upon discovery of the Data Breach, and in doing so unreasonably delayed informing Plaintiff and the Class about the Data Breach when

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Defendant knew or should have known that the Data Breach had occurred.

83. As a result of the violation of RCW § 19.255.010(2), Plaintiff and Class members have been damaged and, pursuant to RCW § 19.255.010(13), are entitled to recover damages and an injunction, enjoining Defendant from their unlawful practices.

SEVENTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA CUSTOMER RECORDS ACT, CALIFORNIA CIVIL CODE §§ 1798.80, *ET SEQ.*

84. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the California Subclass.

85. Defendant is a "business" within the meaning of California Civil Code § 1798.80(a).

86. Plaintiff and each member of the California Subclass are "individuals" within the meaning of California Civil Code § 1798.80(c).

87. California Civil Code § 1798.81.5 provides that a business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

88. Plaintiff and California Subclass members provided Personal Information to Defendant that constitutes computerized data and includes Personal Information that is owned, licensed, or maintained by Defendant.

89. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

90. Defendant's failure to have reasonable measures in place to secure the Personal Information was grossly negligent.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

91. Defendant violated the Customer Records Act by failing to notify California residents in the most expedient time possible and without unreasonable delay. Upon learning of the Data Breach, Defendant failed to disseminate the required notification to Plaintiff and the other California Subclass members.

92. Defendant's notification of the Data Breach was insufficient, misleading, and not compliant with the law.

93. California law gives the protection of its citizens' privacy the highest priority. Article 1, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursing and obtaining safety, happiness and privacy."

94. California's common law and statutory scheme also recognizes and protects California residents' right of privacy. For example, California Civil Code § 1798.81.5(a) states: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information."

95. California citizens' rights to privacy have been compromised and infringed by the Defendant's acts and omissions.

96. Under California Civil Code § 1798.84, any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.

97. As a result of Defendant's violations of the Customer Records Act and the Data Breach, Plaintiff and the other California Subclass members were injured and incurred actual harm and damages. Plaintiff and the other Subclass members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

EIGHTH CAUSE OF ACTION
VIOLATION OF THE UNFAIR COMPETITION LAW, BUSINESS & PROFESSIONS CODE § 17200, *ET SEQ.*

98. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the California Subclass.

99. California's Unfair Competition Law, California Business & Professions Code § 17200, *et seq*. (the "UCL") provides that unfair practices include, but are not limited to, "any unlawful, unfair or fraudulent business act[s] or practice[s]."

100. Defendant engaged in activities that constitute unlawful, unfair and fraudulent business practices prohibited by the UCL.

101. Defendant knew or should have known that its failure to implement and maintain reasonable security procedures and practices to protect Plaintiff's and the other California Subclass members' Personal Information was unlawful, unfair, and fraudulent. Defendant willfully ignored the clear and present risk of a security breach of their systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach. Defendant benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

102. Defendant's conduct is unlawful because it violates the statutes referenced herein, and constitutes negligence and negligence *per se*.

103. Defendant's conduct was unfair because it violates established public policy established by the FTC and California law governing the security and privacy of consumers' personal information. Defendant's conduct is also immoral, unethical, oppressive or

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

unscrupulous and causes injury to consumers that outweighs its benefits. Any benefit to consumers of Defendant's services is outweighed by the harm to consumers of the disclosure of their Personal Information. Consumers could not have avoided this harm themselves.

104. Defendant's conduct is fraudulent because it made representations and omissions on its websites about the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Defendant's security measures were also unable to detect suspicious and unauthorized activity until it was offered for sale on the Internet.

105. Plaintiff and the other California Subclass members have suffered actual damages including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach.

106. Plaintiff's and the other California Subclass members' injuries were proximately caused by Defendant's violations of the UCL. Defendant acted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

107. Plaintiff and the other California Subclass members are also entitled to injunctive relief in the form of deletion and destruction of data, greater security practices and protocols, and training and compliance with industry standards governing data security.

NINTH CAUSE OF ACTION
CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, CAL. CIV. CODE §§ 1750, *ET SEQ.*

108. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the California Subclass.

109. Defendant engaged in following prohibited conduct in violation of the California Consumer Legal Remedies Act, Cal. Civ. Code § 1770 (the "CLRA"), among others:

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

a. Misrepresenting the source, sponsorship, approval, or certification of goods or services;

b. Representing that goods or services have characteristics that they do not have;

c. Representing that goods or services are of a particular standard, quality, or grade when they are not;

d. Advertising goods or services with intent not to sell them as advertised; and

e. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

110. Defendant's representations and omissions were material and likely to mislead a reasonable consumer about the quality of Defendant's data security and ability to protect Personal Information in the provision of cellular phone and data services.

111. Plaintiff and the other California Subclass members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach. Plaintiff is providing the statutory notice required under the CLRA and will amend this claim to assert a request for damages at the end of the statutory waiting period if Defendant does not take corrective action.

TENTH CAUSE OF ACTION

CALIFORNIA CONSUMER PRIVACY ACT, CIVIL CODE §§ 1798.100, ET SEQ.

112. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein. Plaintiff asserts this claim on behalf of the California Subclass.

113. At all times during Plaintiff's and Subclass members' interactions with Defendant, Defendant were fully aware of the confidential and sensitive nature of Plaintiff's

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

and Subclass members' PI that they provided to Defendant.

114. Defendant's relationship with Plaintiff and Subclass members was governed by terms and expectations that Plaintiff's and Subclass members' PI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

115. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Subclass members' PI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Subclass members' confidence, and without their express permission.

116. Through the above-detailed conduct, Defendant violated California Civil Code section 1798.150 by failing to protect Plaintiff's and Subclass members' nonencrypted PI from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

117. As a proximate result of such unauthorized disclosures, Plaintiff's and Subclass members' PI, including, among others, names, dates of birth, Social Security numbers, and account information, was subjected to unauthorized access and exfiltration, theft, and disclosure.

118. Plaintiff seeks injunctive relief on behalf of the Subclass as well as other equitable relief. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiff and Subclass members. Plaintiff and Subclass members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Classes.

119. In accordance with Civil Code section 1798.150(b), Plaintiff will serve Defendant with notice of violation of Civil Code section 1798.150(a) and a demand for relief. If Defendant fails to properly respond to Plaintiff's notice letter or agree to timely and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

adequately rectify the violations detailed above, Plaintiff will also seek actual, punitive, and statutory damages, as well as restitution, attorneys' fees and costs, and any other relief the Court deems proper.

ELEVENTH CAUSE OF ACTION

DECLARATORY JUDGMENT

120. Plaintiff realleges each and every allegation above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

121. Plaintiff and the Class have stated claims against Defendant for common law torts and statutory violations.

122. Defendant failed to fulfill its obligations to provide adequate and reasonable data security measures for the Personal Information of Plaintiff and the Class, as evidenced by the Data Breach.

123. As a result of the Data Breach, Defendant's systems are more vulnerable to access by unauthorized parties and require more stringent measures to be taken to safeguard the Plaintiff's and Class members' Personal Information going forward.

124. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide data security measures that will adequately protect Plaintiff's and Class members' Personal Information.

125. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent, industry-standard data security practices to provide reasonable protection and security to Plaintiff and Class members' Personal Information. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with its obligations, and that Defendant must implement and maintain reasonable data security measures on behalf of Plaintiff and the Class to comply with its data security obligations.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and on behalf of the Class and California Subclass, prays for relief as follows:

A. For an order certifying the Class and California Subclass and appointing Plaintiff as class representative;

B. Awarding monetary and actual damages and/or restitution, as appropriate;

C. Awarding punitive damages, as appropriate;

D. Awarding declaratory and injunctive relief as permitted by law or equity to ensure that the Class and California Subclass have an effective remedy, including enjoining Defendant from continuing its unlawful practices;

E. Prejudgment interest to the extent allowed by the law;

F. Awarding all costs, including expert fees and attorneys' fees, expenses and costs of prosecuting this action; and

G. Such other and further relief as the Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 31st day of August, 2021.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 N. 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 206-816-6603
Facsimile: (206) 319-5450

Laurence D. King, *pro hac vice forthcoming*
Email: lking@kaplanfox.com
Matthew George, *pro hac vice forthcoming*
Email: mgeorge@kaplanfox.com
KAPLAN FOX & KILSHEIMER LLP
1999 Harrison Street, Suite 1560
Oakland, California 94612
Telephone: (415) 772-4700
Facsimile: (415) 772-4707

David Silver, *pro hac vice forthcoming*
Email: dsilver@silvermiller.com
SILVER MILLER
11780 West Sample Road
Coral Springs, FL 33065
Telephone: (954) 516-6000

Attorneys for Plaintiff and the proposed Class and Subclass

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com